

NOV 6 2007

MEMORANDUM FOR DEPARTMENT OF DEFENSE EXECUTIVE AGENT FOR
INFORMATION TECHNOLOGY STANDARDS
(ATTN: THE CHAIR, INFORMATION TECHNOLOGY STANDARDS
COMMITTEE)

SUBJECT: Department of Defense Information Technology Standards Registry Baseline Release
07-3.0

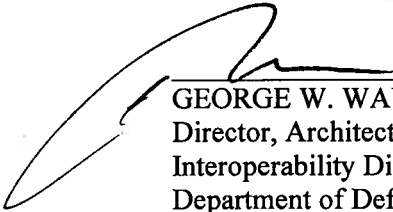
References: (a) DoD Directive 4630.5, Interoperability and Supportability of Information
Technology (IT) and National Security Systems (NSS), May 5, 2004
(b) DoD Directive 5101.7, DoD Executive Agent for Information Technology
Standards, May 21, 2004

The DoD Information Technology (IT) Standards Registry (DISR) has been updated from
Baseline Release 07-2.0 to DISR Baseline Release 07-3.0 in accordance with Reference (a).
According to Reference (b) the DISR baseline is updated periodically to ensure the DoD
capabilities for building and buying IT systems are based on a current and effective set of IT and
NSS standards.


As Chairs of the Information Technology Standards Oversight Panel (ISOP) and under the
authority of the DoD CIO, we approve the attached changes to the DISR baseline as
recommended by the Information Technology Standards Committee (ITSC). Please post the
approved changes as DISR Baseline Release 07-3.0 for immediate use in DoD IT and NSS
acquisitions and development systems. This Release supersedes Release 07-2.0 and contains IT
and NSS standards needed to support interoperability and a net-centric operational environment.

We also approve the GIG Enterprise Profile for IPv6 Base Standards along with the document
"Implementing DoD IPv6 Standard Profiles and IPv6 Capable Products—Supplemental
Guidance," Version 2.0, dated 1 Aug 2007, and Errata dated 30 August 2007.


Once again we extend our thanks to the members of the ITSC and the Technical Standards
Working Groups for their involvement and contributions to the DoD standards process.



GEORGE W. WAUER
Director, Architecture and
Interoperability Directorate
Department of Defense
Chief Information
Officer/Assistant Secretary
of Defense for Networks and
Information Integration



MICHAEL J. BASLA
Brigadier General, USAF
Vice Director, Command
Control, Communications,
and Computers Systems
Joint Staff



MARK D. SCHAEFFER
Director
Systems and Software
Engineering
Under Secretary of Defense for
Acquisition Technology and
Logistics

Copy to: DoD CIO Executive Board
ITSC Representatives

Attachments:

- a. Changes for DISR Baseline 07-3.0
- b. GIG Enterprise Profile for IPv6 Base Standards

DoD IPv6 Standard Profiles For IPv6 Capable Products Version 2.0

01 August 2007

Prepared by the DISR IPv6 Standards Technical Working Group
POC: Ralph Liguori, Chair IPv6 Standards TWG
E-mail Address: ralph.liguori@disa.mil

Table of Contents

| | |
|---|-----------|
| Executive Summary..... | 4 |
| 1 Introduction..... | 5 |
| 1.1 A Definition of “IPv6 Capable Product” | 5 |
| 1.2 Document Goals and Purpose | 5 |
| 1.3 Target Audience..... | 6 |
| 1.4 Requirement Sources | 7 |
| 1.5 Terminology Used in This Document | 8 |
| 1.6 IPv6 Capable Product Classes | 10 |
| 2 IPv6 Capable Product Requirements | 13 |
| 2.1 Base Requirements | 14 |
| 2.2 IP Layer Security (IPsec) Functional Requirements..... | 15 |
| 2.2.1 RFC 4301 Architecture..... | 17 |
| 2.2.2 IKE Version 2 Support | 17 |
| 2.3 Transition Mechanism (TM) Functional Requirements..... | 18 |
| 2.4 Quality of Service (QoS) Functional Requirements..... | 19 |
| 2.5 Mobility (MOB) Functional Requirements..... | 20 |
| 2.5.1 MIPv6 Capable Node..... | 20 |
| 2.5.2 Home Agent Router | 20 |
| 2.5.3 NEMO Capable Router | 21 |
| 2.5.4 Route Optimization | 21 |
| 2.6 Bandwidth Limited Networks Functional Requirements | 21 |
| 2.6.1 Robust Header Compression (RoHC)..... | 21 |
| 2.6.2 IP Header Compression..... | 22 |
| 2.7 Network Management (NM) Functional Requirements | 22 |
| 2.8 Routing Protocol Requirements | 22 |
| 2.8.1 Interior Router Requirements..... | 23 |
| 2.8.2 Exterior Router Requirements..... | 23 |
| 3 Product Class Profiles..... | 23 |
| 3.1 IPv6 End Nodes | 23 |
| 3.1.1 Host/Workstation Product Class Profile | 23 |
| 3.1.2 Network Appliance Product Class Profile..... | 24 |
| 3.1.3 Server Product Class Profiles | 24 |
| 3.2 IPv6 Intermediate Nodes..... | 26 |
| 3.2.1 Router Product Profile..... | 26 |
| 3.2.2 Layer-3 (L3) Switch Product Profile | 27 |
| 3.2.3 Information Assurance (IA) Device Product Profile | 27 |
| 4 IPv6 Capable Software..... | 29 |
| 4.1 Application Programming Interface (API) Characteristics | 29 |
| 4.2 Software Requirements..... | 30 |
| Appendix A: References | 31 |
| Appendix B: Glossary | 33 |
| Appendix C: Requirements Summary Table | 34 |

Acknowledgements44

Executive Summary

This document provides the engineering-level definition of “IPv6 Capable” products necessary for interoperable use throughout the US Department of Defense (DoD). This content has been synthesized from multiple sources including DoD policy statements [1] [2] [8], DoD Information Technology Standards Registry (DISR) requirements [3], DoD IPv6 Transition Office (DITO) guidance [4] [5] and Internet Engineering Task Force (IETF) published requirements. The term “IPv6 Capable Product”, as used in this document, means any product that meets the minimum set of mandated requirements, appropriate to its Product Class, necessary for it to interoperate with other IPv6 products employed in DoD IPv6 networks. Version 1.0 of this Standard Profiles document was approved by the DoD Information Standards Oversight Panel (ISOP) under the authority of the DoD CIO to “provide guidance to DoD Components and Services responsible for procuring/acquiring IPv6 Capable GIG products” [6]. Final review and approval of this revision will be similarly documented.

The document is intended to assist several communities of interest in executing their responsibilities for preparing DoD systems and networks to be IPv6 Capable. The topic is rather technical in nature, and requires some background understanding of Internet protocols but the goal of this document is to organize and summarize the requirements included by reference for the convenience of the reader. The authors hope that each type of reader referenced below finds it useful:

1. Acquisition officers may use this document as a reference when they develop specific product and system requirements; for their purposes, the listing of RFCs and other specifications herein may be sufficient.
2. Testing organizations may use this document as an outline for detailed test plans appropriate to each product class described based on the details in this document along with reference to the specifications and other technical material cited.
3. DoD systems developers and their management as well as vendors may use this document as an additional check on their systems architecture, design and implementation to assure that their products will be interoperable with other network elements and that their products will be ready for DoD IPv6 Capable testing.

This document as a whole defines a set of DoD IPv6 Standard Profiles (Profiles) for IPv6 Capable Products of various classes of equipment or software, and variety of IPv6 network roles. First, Product Classes are defined that will be used in the document to group products according to their role in a network architecture. Then the Base Requirements that apply to all IPv6 Capable Product Classes are defined. Several Functional Requirements blocks are defined for specific functions performed by some products. Finally, Product Class Profiles are defined in terms of the Base Requirements and Functional Requirements.

[References](#), a [Glossary](#) and an [Appendix](#) with a summary of the requirements in tabular form are provided at the end of the text.

1 Introduction

1.1 A Definition of “IPv6 Capable Product”

A Memorandum issued by the Assistant Secretary of Defense – Networks and Information Integration (ASD(NII)) entitled “Internet Protocol Version 6 (IPv6) Policy Update” [8] states that:

“IPv6 ‘capable’ is defined as a system or product capable of receiving, processing and forwarding IPv6 packets and/or interfacing with other systems and protocols in a manner similar to IPv4. Criteria to be considered IPv6 capable are: conformant with the IPv6 standards profile contained in the DoD IT Standards Registry (DISR); maintaining interoperability in heterogeneous environments with IPv4; commitment to upgrade as the IPv6 standard evolves; and availability of contractor/vendor IPv6 technical support.”

Version 1.0 of this document was approved by the ISOP [6] as representing the “IPv6 Profile” taking the place of the Generic IPv6 Profile in the DISR. Thus, this document provides a detailed definition of an “IPv6 Capable Product” by enumerating the requirements that must be met by a particular product for it to be considered IPv6 Capable.

While other terms such as “IPv6 Ready” or “IPv6 Compliant” have been used in other contexts, the term “IPv6 Capable Product” as it is defined in this document should be used in conjunction with a citation of this document to be clear about what is required. The term “IPv6 Capable Product”, as used in this document, means any product that meets the minimum set of mandated requirements, appropriate to its Product Class, necessary for it to interoperate with other IPv6 products employed in DoD IPv6 networks. The term “IPv6 Capable Node” is used throughout this document to refer to an arbitrary IPv6 Capable Product.

1.2 Document Goals and Purpose

This document provides a technical and standards based definition of interoperability requirements for IPv6 Capable Products to be used in U.S. Department of Defense (DoD) networks. This content has been synthesized from multiple sources including DoD policy statements [1] [2] [8], DoD Information Technology Standards Registry (DISR) requirements [3], DoD IPv6 Transition Office (DITO) guidance [4] [5] and Internet Engineering Task Force (IETF) published requirements. Version 1.0 of this document was reviewed and approved by the ISOP as guidance for the acquisition of IPv6 Capable Products [6] and when approved, this version will replace Version 1.0.

RFC 4294 “IPv6 Node Requirements” published by the IETF in April, 2006 has been an essential guide in the preparation of this document. The following goal statement from that RFC can also serve as the basis for the goals of this document:

“The goal of this document (RFC 4294) is to define the common functionality required from both IPv6 hosts and routers. Many IPv6 nodes will implement optional or additional features, but this document summarizes requirements from other published Standards Track¹ documents in one place.

This document tries to avoid discussion of protocol details, and references RFCs for this purpose. This document is informational in nature and does not update Standards Track RFCs.

Although the document points to different specifications, it should be noted that in most cases, the granularity of requirements are smaller than a single specification, as many specifications define multiple, independent pieces, some of which may not be mandatory.”

Likewise, this document does not intend to define or mandate new requirements nor to unduly restrict use of optional requirements, but to summarize the requirements for IPv6 Capable Products. To facilitate interoperability:

1. A device should not rely upon or assume the implementation of optional features in other devices;
2. A device should, when feasible, implement optional features that other relevant devices are likely to depend upon;
3. While a device may implement any optional features not specifically forbidden in this document, care should be taken to avoid anything that would interfere with another device implementing permitted features.

1.3 Target Audience

The document is intended to assist several communities of interest in executing their responsibilities for preparing DoD systems and networks to be IPv6 Capable. The topic is rather technical, and requires some background understanding by the reader of the RFCs and other references cited, but the goal of this document is to organize and summarize the requirements included by reference for the convenience of the reader. The authors hope that the document is useful to several categories of users as described in the following paragraphs.

Contracts and Acquisition

Acquisition officers and others writing purchasing and contract language may use this document as a reference when they develop specific product and system requirement

¹ Standards Track is an IETF term indicating that an RFC is published with the intention that it will become an Internet Standard when mature and widely implemented. An RFC is usually published as a “Proposed Standard” and is promoted to “Draft Standards” before being considered for Internet Standard status. Further explanation of this process can be found in RFC 2026.

text. For their purposes, this document aims to adequately summarize the technical requirements such that it is sufficient (with the citation of RFCs and other specifications referenced by this document) to specify the minimal requirements for products to be IPv6 Capable.

Testing and Certification Organizations

DoD components will rely upon testing organizations including the Joint Interoperability Test Command (JITC) to evaluate vendor products and DoD systems as IPv6 Capable. These testing organizations may use this document as an outline and starting point for the development of detailed test plans appropriate to each product class. They will need to go beyond the summary level of this document through reference to the specifications and other technical material cited.

Developers

The engineers and managers responsible for systems development by DoD and vendor organizations may use this document as an additional check on interpretation of the specifications and other technical material cited to develop systems architectures, designs and implementations to assure that their products will be IPv6 Capable. By following the requirements documented herein, they will increase the probability that the systems they build will be interoperable with other DoD IPv6 Capable network elements and will be ready for DoD testing.

1.4 Requirement Sources

The immediate reference for requirements in this document is the Defense Information Systems Registry (DISR). The DISR is a snapshot of the state-of-practice for technical publications being tracked by DISA for inclusion in profiles for products to be acquired by DoD. These technical publications come from a number of sources, primarily external Standards Development Organizations (SDOs) and are reviewed and considered by the DoD IT Standards Committee (ITSC) and a number of DoD IT Standards Technical Working Groups (TWGs). When standards are sufficiently mature, they are added to the DISR database.

In particular, IPv6 specifications and related standards are published by the Internet Engineering Task Force (IETF) as Requests for Comments (RFCs). These documents are reviewed and analyzed by members of the IPv6 Standards TWG, and considered for mandatory or optional use in DoD systems and networks when they are stable and mature and determined to be appropriate requirements for use by DoD. Each of the RFCs cited in the DISR and in this document is included by reference in its entirety, except where this document notes exceptions or extensions. RFCs can be freely obtained through the [RFC Editor](#) by searching on the RFC number or keywords.

The DISR is updated 3 times a year after due consideration of new and replacement RFCs by the IPv6 Standards TWG. This document is coordinated with the content of

the DISR database at the time of its publication, and will be updated and republished as necessary to maintain this correspondence.

In February 2007, the National Institute of Standards and Technology (NIST) released a draft for public comment entitled “A Profile for IPv6 in the U.S. Government” [9]. That document is intended for U.S. Government environments exclusive of the DoD. While we have worked with the authors of that document to minimize differences between the documents, they will remain parallel efforts for the foreseeable future. Per the cited DoD policy statements [1] [2] [8] DoD acquisition of products for IPv6 deployment should follow this document.

1.5 Terminology Used in This Document

The DISR database and IETF RFCs use different terminology to describe requirements. RFCs and other technical publications referenced in the DISR as standards are assigned to one of 3 statuses:

EMERGING: An EMERGING standard is a new or evolving standard that is likely to eventually become a MANDATED standard.

MANDATED: A MANDATED standard is a stable and mature standard that can be cited as a requirement in acquisition. One of the considerations for determining maturity of a standard is the existence of vendor implementations.

RETIRED: A standard that has been replaced by a newer standard or otherwise determined to be no longer appropriate for use in DoD systems is a RETIRED standard.

Additionally, RFCs or other publications can be referenced in the DISR as **INFORMATIONAL/GUIDANCE** meaning that they provide useful information that is not a standard.

IETF terminology for use in RFCs is defined in RFC 2119 including the terms MUST, SHOULD, and MAY. To provide a common lexicon, the following six terms used in this document are to be interpreted as follows:

MUST: This term indicates an imperative; the requirement is essential to IPv6 capability and interoperability. This level of requirement is indicated in the DISR by MANDATED. Synonyms used in other contexts include SHALL or REQUIRED.

MUST NOT: This term indicates an absolute prohibition of a behavior. A synonym is SHALL NOT.

SHOULD: This term indicates a desirable or expected course of action or policy that is to be followed unless inappropriate or cost-prohibitive for a particular circumstance. This corresponds to the EMERGING² level in the DISR.

SHOULD NOT: This term is used to indicate that the particular behavior is discouraged though not prohibited. There may be valid reasons in particular circumstances when the behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing.

MAY: This term denotes the permissive or that an item is truly optional. An implementation which does not include a particular option **MUST** interoperate with another implementation which does include the option. In the same vein, an implementation which does include a particular option **MUST** be prepared to interoperate with another implementation which does not include the option (in both cases without the feature the option provides). Normally standards that a product **MAY** follow would be listed in the DISR as INFORMATIONAL.

SHOULD+: This term indicates a near-term goal for technology insertion that is strongly expected to be elevated to a **MUST** or **MANDATED** in the near future. **SHOULD+** means a strongly recommended and expected course of action or policy that is to be followed unless inappropriate for a particular circumstance. This term is normally associated with an EMERGING specification in the DISR.

IPv6 is defined by an active and evolving set of RFCs. In addition to new emerging standards, existing standards are frequently updated by RFCs that extend or elaborate the standards, and on occasion standards may be rendered obsolete by revised RFCs. In IETF practice, once published, an RFC is never updated; the technical material it defines can only be changed by publication of another RFC. The [RFC Editor](#) web page tracks all RFCs, and relates them to other RFCs that update or obsolete them.

The obsolescence and replacement of RFCs by new RFCs complicates a simple and clear definition of the mandatory requirements in this Standard Profiles document. There will be a period of time during which commercially available products may support either or both of the versions of the standard. In some cases the requirement is to support the *function*, preferably complying with the emerging replacement RFC but at least according to the previously published RFC. In these situations, the old and new standards will be discussed together in this document with exceptions or conditions noted, to provide clear guidance to vendors for implementation and testing.

Throughout this document the terms “support” and “implement” as well as other forms of the words such as “supported”, “implementation”, etc. are used to indicate that a requirement or function is available in a product. In other words, the compliant product is capable of providing the function. For example, if a product class **MUST** support

² A standard that is listed in DISR as **MANDATED** could also be used in **SHOULD**, **SHOULD+** and **MAY** clauses.

MLDv2 as defined in RFC 3810, a compliant product of that class meets the requirements in that RFC to provide MLDv2 function. This does not imply that the available function will be actively used. The terms “deployment” and “use” as well as other forms of those words indicate active operation of an available capability or function.

Note also that some requirements clauses may be applied conditionally. The language in these instances is intended to be self-explanatory, and stated as simply as possible to capture the technical nuances, for example as used in Section 3.1.1:

“An IPv6 Capable Host/Workstation...Conditionally, MUST implement MIPv6 Capable Node Functional Requirements (Section 2.5.1) IF intended to be deployed as a Mobile Node.”

This should be read to mean that the requirement to support the sections of the RFCs for MIPv6 Mobile Node functionality would not be mandatory for all IPv6 Capable Host/Workstation Products, but is mandatory for products that are intended to operate as a Mobile Node in a MIPv6 deployment.

1.6 IPv6 Capable Product Classes

Before examining detailed requirements it would be useful to frame the discussion by defining the classes of IPv6 Capable Products. The terminology used in the IPv6 base specification [RFC 2460] only defined two very general classes of nodes. Describing the requirements for a specific IPv6 Capable product using those broad classes would require complex exceptions and explanations to distinguish among different products. This Standard Profiles document groups IPv6 Capable Products into a small number of Product Classes convenient for defining common requirements. IPv6 Capable Products are classified according to their architectural and functional role in an IPv6 network:

- **End Node:** A node processing IPv6 packets addressed to the node itself or originating IPv6 packets with a source address of the node itself.
 - **Host/Workstation:** PC or other end-user computer or workstation running a general purpose Operating System (OS) such as UNIX®^A, Linux®^B, Windows®^C, or a proprietary operating system that is capable of supporting multiple applications. A Host/Workstation can be viewed as a hardware platform combined with its OS; however the embodiment of the IPv6 Capability in the OS is generally independent of the platform.³ A

³ In fact the particular hardware is usually irrelevant; for example, Microsoft Vista running on any PC has the same IPv6 capabilities, and a Host/Workstation should be considered as a combination of the platform and the Operating System. The PC running Vista in this case, whether HP, Dell or custom-built has no IPv6 capability of its own independent of the Software loaded. There can be exceptions, for example a platform with a hardware implementation of the IP stack, where the IPv6 features may be different. This note may apply to products in any of the Product Classes.

Host/Workstation typically has a single user, with a local (console) login, and is generally managed by the end-user (or the end-user organization support team, rather than the Internet Service Provider (ISP) or other third party.)

- **Network Appliance:** Simple end nodes such as cameras, sensors, automation controllers, networked phones or adapters such as Circuit-to-Packet (CTP) devices, typically with an embedded operating system and specialized software for limited applications. A Network Appliance is typically managed by an end-user, but may support more than one concurrent user remotely via a Web browser interface.
- **Server:** End Nodes with one or more server-side applications (for example DHCPv6, DNS, NTP, E-mail, FTP, HTTP, web server, storage server or database) to support clients in the network. Servers are usually managed by network administrators or operated by a third party such as an ISP or other vendor.
 - A **Simple Server** is similar to a Network Appliance, with an embedded operating system and contains specialized software for limited applications for a small number of concurrent clients via a web browser interface or other protocol with a client application. Examples of simple servers are stand-alone network print servers, storage servers, Session Initiation Protocol (SIP)⁴ servers, a “web camera” appliance that serves pictures via an embedded web server, and a network time server appliance that solely functions to serve NTP requests.
 - An **Advanced Server** typically runs a general purpose operating system such as UNIX, Linux, Windows, or a proprietary operating system and is capable of serving any number of applications to many concurrent clients. Examples include Domain Name Servers, web hosting servers and database servers.
- **Intermediate Node:** A node that forwards IPv6 packets not explicitly addressed to the node itself.⁵
 - **Router:** An Intermediate Node that forwards packets based on paths discovered using routing protocols. A router typically has a small number of ports to interconnect several networks, in particular to connect a Local Area Network (LAN) to a Wide Area Network (WAN). A Router implements complex control plane functions, including routing protocols such as Open Shortest Path First (OSPF) and Border Gateway Protocol

⁴ See RFC 3261 Session Initiation Protocol for more information on SIP

⁵ Please note that an Intermediate Node may also act as an End Node for Network Management and other protocols, and must conform to End Node functionality for IPv6 packets addressed to an IPv6 address of the node itself.

(BGP) which are typically implemented in software run on a general purpose CPU.

- **Layer-3 Switch:** An Intermediate Node that forwards IPv6 packets at switching speeds usually through the use of special purpose dedicated hardware. A Layer-3 Switch typically has a higher port density than a Router and is intended to interconnect end-nodes in a LAN environment. A Layer-3 Switch may have some limited layer-3 control plane (management or routing) functions but is primarily a data plane device.
- **Information Assurance Device:** An Intermediate Node that performs a security function by filtering or encrypting network traffic, and which may block traffic when security policy dictates. For example a Firewall, Intrusion Detection System, Authentication Server, Security Gateway or VPN. A Router or L3 Switch may also act as an Information Assurance Device when it incorporates these functions.
- **IPv6 Capable Software:** a product that implements functions available to end-users, network nodes or other software, when installed on an appropriate hardware platform. Section 4 of this document introduces some concepts for the evaluation of pure software IPv6 Capable products (operating systems or applications) but a full definition of IPv6 Capable Software Product Classes is deferred to a future revision of this document.

Some of the terms used in this document for defining Product Classes have been used with different definitions in the networking industry, but throughout this document and in references to this document, the terms are intended to be used as defined above. In particular the term Network Appliance has been used for a variety of End Node and Intermediate Node products, and is the name of a storage solutions company.

We have attempted to make the distinctions between Product Classes as objective as possible, but some of the differences are subject to interpretation, in particular the classification of a Server product as “Simple” or “Advanced”. It is essential that a vendor come to agreement with the testing organization (JITC for example) on proper classification of their product before testing. The testing organization and the Chairman/POC of the DISR IPv6 Standards TWG can be of assistance in classifying products that don’t obviously fit one of the Product Classes. Many products include other interfaces in addition to the IPv6 interface, such as a Voice-over-IP (VOIP) device or Circuit-to-Packet (CTP) device. Such a device can be evaluated as a “black box” from its IPv6 interface, without regard to other internal or external non-IPv6 interfaces.

The following table summarizes the Product Class definitions and characteristics to help with the classification of specific products. For example, if the product is an End Node, managed by the End-User organization, accessed by a single user through a local interface rather than remotely via a Web interface, it is best identified as a Host/Workstation.

| | Host/ Workstation | Network Appliance | Advanced Server | Simple Server | Router | Layer 3 Switch | Information Assurance Device |
|----------------------------|-----------------------|----------------------|--------------------|------------------|----------|-------------------|------------------------------------|
| End Node | Yes | Y | Y | Y | Optional | O | O |
| Intermediate Node | No | N | N | N | Y | Y | Y |
| End-User Managed | Y | Y | N | N | N | N | N |
| Web Access | N | O | O | O | O | O | O |
| Local login or console | Y | O | O | O | O | O | O |
| Loadable or Embedded | Loadable ⁶ | Embedded | O | E | O | O | O |
| Number of Applications | Many | Few | 1 to M | F | n/a | | |
| Number of Users | 1 | 1 to F | M | F | | | |
| Network Interconnection | n/a | | | | Y | N | n/a |
| Port Density | | | | | Low | High | |
| Complex Control Plane | | | | | Y | N | |
| IA Function | | | | | O | O | |

Table 1-1: Product Class Summary

2 IPv6 Capable Product Requirements

This section identifies the specifications that will be used to define the requirements for the Product Classes outlined above. These specifications are organized into several functional categories. First, the Base Requirements are defined, comprising the standards that will (with minor exceptions) apply equally to all Product Classes. Then, a set of Functional Requirements categories are defined, which will be used as “building blocks” to construct the detailed Product Class Profiles in Section 3.

⁶ A Host/Workstation is typically “loadable” although in practice, some systems may be preloaded by an administrator with the end user restricted from loading additional software.

Specific requirements in the RFCs cited in the Base or Functional Requirements may apply to IPv6 End Nodes and IPv6 Intermediate Nodes or may apply differently to each class. The reader may read the cited RFCs for a more detailed understanding of the specific requirements. Extensions, restrictions and exceptions with respect to the Product Classes defined in this document can be found in Section 3.

2.1 Base Requirements

These Base Requirements are the core of interoperability requirements for IPv6 Nodes.

- All IPv6 Nodes MUST conform to RFC 2460⁷, Internet Protocol v6 (IPv6) Specification; this is the fundamental definition of IPv6.
- All IPv6 Nodes MUST implement RFC 4443, Internet Control Message Protocol (ICMPv6).
- All IPv6 Nodes MUST implement RFC 2461, Neighbor Discovery for IPv6, as appropriate to their role as an IPv6 End Node or IPv6 Intermediate Node.
- All IPv6 Nodes MUST operate with the default minimum Path MTU (PMTU) size of 1280 octets as defined in RFC 2460. All IPv6 Nodes SHOULD support a minimum PMTU of 1500 to allow for encapsulation. All IPv6 Nodes except Network Appliance or Simple Server MUST implement RFC 1981, Path MTU Discovery for IPv6.
- All IPv6 Nodes MUST provide manual or static configuration of its IPv6 interface address(es).
- All IPv6 Nodes MUST support at least one autonomous method for discovering its own unique IPv6 interface address(es), either RFC 2462, IPv6 Stateless Address Auto-configuration (SLAAC) or the client side of RFC 3315, DHCPv6. DHCPv6 provides for a stateful equivalent to SLAAC. The two methods are complementary but not mutually exclusive.
- All IPv6 Nodes supporting either autonomous method MUST have the means to disable the autonomous method to force manual or static configuration of addresses (e.g. the user can disable the “Creation of Global and Site-Local Addresses” as described in Section 5.5 of RFC 2462 on an IPv6 Node that supports SLAAC). However link-local address configuration and Duplicate Address Detection (DAD) MUST NOT be disabled.
- All IPv6 Nodes MUST support the IPv6 Addressing Architecture as defined in:
 - RFC 4291, IPv6 Addressing Architecture
 - RFC 4007, Scoped Address Architecture (All IPv6 addressing plans MUST use this standard definition for scoped addressing architectures, however support for zone indexes is optional)
 - RFC 4193, Unique Local IPv6 Unicast Addresses (Replaces the site-local address with a new type of address that is private to an organization, yet unique across all of the sites of the organization)

⁷ Recently a security vulnerability with Routing Header type 0 (RH0) has been noted, and an Internet Draft [10] is circulating that proposes this option be deprecated.

- All IPv6 Nodes MUST implement Multicast Listener Discovery (MLD)
 - Neighbor Discovery (ND) is a core feature of IPv6, analogous to ARP in IPv4, therefore a fundamental requirement for IPv4 parity. ND requires the use of Multicast; therefore ALL IPv6 Capable products will be using Multicast. In addition, switches may include the "MLD Snooping" feature that will block multicast addresses that are not registered with MLD. This means that products lacking MLD support cannot guarantee that ND will work in all deployments.
 - At a minimum all nodes MUST follow RFC 2710, Multicast Listener Discovery for IPv6.
 - All IPv6 Nodes (except L3 Switches, Information Assurance Device, Network Appliance and Simple Server) MUST support the extended MLDv2 as in RFC 3810, Multicast Listener Discovery Version 2 (MLDv2) for IPv6.⁸
- All IPv6 Nodes conditionally MUST support a connection technology (link layer) that can carry IPv6 packets, consistent with its intended deployment. When using a connection technology with a published "IPv6 over" standard the device MUST follow the corresponding standard for interoperability across that connection technology:
 - RFC 2464, Transmission of IPv6 Packets over Ethernet Networks;
 - RFC 2492, IPv6 over ATM Networks;
 - RFC 2472, IP Version 6 over PPP;
 - RFC 3572, IPv6 over MAPOS (Multiple Access Protocol over SONET/SDH).
 - RFC 2467, Transmission of IPv6 Packets over FDDI Networks;
 - RFC 2491, IPv6 Over Non-Broadcast Multiple Access (NBMA) Networks;
 - RFC 2497, Transmission of IPv6 Packets over ARCnet Networks;
 - RFC 2590, Transmission of IPv6 Packets over Frame Relay Networks Specification;
 - RFC 3146, Transmission of IPv6 over IEEE 1394 Networks;
 - RFC 4338, Transmission of IPv6, IPv4 and Address Resolution Protocol (ARP) Packets over Fibre Channel.

2.2 IP Layer Security (IPsec) Functional Requirements

Security is a complex topic and the role of IP Layer Security (IPsec) within the overall DoD approach to security is still evolving. The DoD transition to IPv6 requires IPsec as part of the toolkit to build secure networks. There are several dimensions to the treatment of IPsec in this set of profiles:

1. For IPsec to be useful as a security tool it must be generally available and devices in the network cannot interfere with its use;

⁸ RFC 3590 addresses the incompatibilities between MLD and Neighbor Discovery, and may be added as an emerging standard.

2. A node's responsibilities with respect to IPsec must be considered in the architectural context; a Router or Switch does not perform IPsec as part of normal traffic forwarding, however it may implement IPsec when it is acting as an End Node in some deployments for network management and in routing protocols; furthermore, when IPsec is imposed on the traffic being forwarded by an Intermediate Node, that Node becomes a special-purpose IA device functioning as a Security Gateway;
3. Products are required to support IPsec so that it is available for use; however, its activation in deployments at this time is optional;
4. NSA opinion that any device implementing encryption with IPsec is an Information Assurance (IA) device subject to FIPS and NIAP certification may be an impediment to wide vendor support but this is beyond the scope of this document. NIST publication [6] on this subject implies that a vendor may rely on previously approved and available cryptographic modules integrated with their product to avoid certification of their product set.

After due consideration of the above points, the IPv6 Standards TWG consensus was to maintain the strong requirement for IPsec at the current published standards as was stated in Version 1.0. The intention is to prevent the proliferation of IPsec deficient products that may interfere with DoD ability to fully utilize IPsec. The Product Class Profiles in Section 3 identify which Product Classes **MUST** be IPsec Capable; however all IPv6 Capable products **SHOULD+** be IPsec Capable. IPsec Capable requirements are:

1. IPsec Capable products **MUST** support the current RFC 4301 Architecture as defined in Section 2.2.1.
2. IPsec Capable products **MUST** support Manual Keying and **MUST** support Internet Key Exchange Version 2 (IKEv2), as defined in Section 2.2.2.
3. IPsec Capable products **SHOULD** support RFC 3971, SEcure Neighbor Discovery (SEND) and RFC 3972 Cryptographically Generated Addresses (CGAs)⁹.
4. IPsec Capable products **SHOULD** support RFC 3041, Privacy Extensions for Stateless Address Auto configuration in IPv6.

A waiver process outside the scope of this document may be available (as determined by DoD component) to allow use of a product that does not at this time support IPsec where required by its Product Class Profile.

⁹ There are some intellectual property rights concerns with CGA and use of CGA in SEND; although the rights are offered on a "Royalty-Free, Reasonable and Non-Discriminatory License to All Implementers", the fact that a license is required may hinder adoption by some vendors.

2.2.1 RFC 4301 Architecture

A set of RFCs defining the Security Architecture for IP and supporting protocols was published in November 1998, and became the de facto standard for security in IPv6 products (RFC 2401 et al, referred to as the RFC 2401 Architecture). This set of standards was rendered obsolete (for the most part) by a set of revised standards in December 2005 (RFC 4301 et al, referred to as the RFC 4301 Architecture).

All IPv6 Nodes implementing IPsec RFC 4301 Architecture **MUST** support the Security Architecture for the Internet Protocol as defined in RFC 4301 and as well:

- **MUST** support the Encapsulating Security Payload (ESP) defined in RFC 4303;
- **SHOULD** support RFC 4302, IP Authentication Header (AH);
- **MUST** implement ESP and AH cryptography as defined in RFC 4305¹⁰, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH).

IPv6 Nodes **SHOULD+** support the cryptographic algorithms for IPsec and IKE according to the options defined in RFC 4869, Suite B Cryptographic Suites for IPsec. Conformance with this cryptographic suite subset is strongly recommended to ensure that all IPsec implementations for DoD approved products support an interoperable set of options. This RFC does not introduce new requirements, but merely clarifies a minimal subset of other referenced RFCs. RFC 4869 **SHOULD+** be used as guidance in the interpretation of the RFCs that it references. Nodes **MAY** support additional cryptographic suites and options where appropriate to the deployment and application but **MUST NOT** depend on other nodes support.

All IPv6 Nodes **SHOULD** support RFC 4304, Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP).

IPv6 Nodes in deployments requiring strong AES based security across wireless links **SHOULD** support RFC 4309, Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP) as this is part of the emerging 802.11i wireless security standard.

2.2.2 IKE Version 2 Support

In conjunction with the IPsec Architecture, some method for key management is required. All IPv6 Nodes need to be interoperable with Product Classes that only support Manual Keying (especially Network Appliances and Simple Servers). Therefore all IPv6 Nodes **MUST** support Manual Keying for IPsec.

¹⁰ RFC 4305 has been obsoleted by RFC 4835, which was published too late for the DISR 07-2.0 change request cycle; it is likely to replace RFC 4305 in the 07-3.0 cycle.

Internet Key Exchange (IKE) was defined in RFC 2409 but has been rendered obsolete by IKE Versions 2 (IKEv2). IKEv2 is simpler to implement, has clearer documentation, is more efficient, has fewer options, and fixes some of the shortcomings in IKEv1. IKEv2 is integral to the RFC 4301 Architecture and some of its advanced features depend on IKEv2 and are not available with the original IKE.

IKE Version 2 (IKEv2) is defined in the following referenced RFCs. An IPv6 Node implementing IKEv2 MUST support:

- RFC 4306, Internet Key Exchange (IKEv2) Protocol
- RFC 4307, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2)

2.3 Transition Mechanism (TM) Functional Requirements

Recognizing that IPv6 Nodes will interoperate with IPv4 for some time, Transition Mechanisms (TMs) will be needed to support interoperability. Like IPsec, TM requirements are dependent on application, deployment and architectural factors. Any IPv6 Capable Node that will interoperate with IPv4 legacy networks or peers MUST provide a way to accommodate the IPv4 base, as there is no capability for IPv4 networks or nodes to interoperate with IPv6. All new nodes being acquired for connection to the DoD GIG must support certain transition mechanisms as described in this section, and may support others.

These mechanisms include dual stack operation, configured and automatic tunneling and translation. RFC 4213, Transition Mechanisms for IPv6 Hosts and Routers, describes several general transition strategies. Each has strengths and weaknesses and would be appropriate to particular architectural situations. To provide maximum interoperability between IPv6 Capable Nodes/Networks and IPv4 nodes/networks the following principles apply:

1. The network (Routers, Switches, Information Assurance Devices and any other intermediate nodes) MUST permit transit of both IPv6 and IPv4 packets. This condition can be met through Dual Stack operation across the network (dual protocol routing) or tunneling at the edge Router.
2. If an IPv6 End Node is required to interoperate with an IPv4-Only End Node, it MUST accept and transmit IPv4 packets. This condition can be met with Dual Stack operation on the platform and dual stack support in the Application.
3. Deployments peering an IPv6-Only Application or IPv6-Only End Node with an IPv4-Only peer MUST include a Translation Method internal to the platform, or through an external translation device as a last resort. While Dual Stack in all nodes (including Dual Stack aware applications) is a preferred solution, some products (Network Appliance or Simple Server) may be IPv6-Only, and for some time IPv4-Only legacy devices will remain.

Translation based on RFC 2766, Network Address Translation – Protocol Translation (NAT-PT) is no longer supported in the IETF community and recent discussions have settled on changing the status of the RFC to *Historic*¹¹. NAT-PT SHOULD NOT be used in operational DoD networks and it would be unlikely that a NAT-PT product would be on the APL.

The Teredo method [RFC 4380] which allows IPv6 traffic to punch through firewalls raises a number of security issues that have been documented [11]. The use of Teredo is strongly discouraged, and will be prohibited in some DoD networks [12].

Use of IPv4 components or a translation solution internal to a product is irrelevant to the IPv6 Capable determination. For example, a translation box that adapts an IPv4-Only legacy device by translation should be evaluated as an IPv6 Host/Workstation, Network Appliance or Server depending on its network deployment. Similarly, a complex product composed of several components may have an internal IPv4 network to connect those components, which is not visible if the “system under test” is considered to be the total complex. Only the externally visible IPv6 interface behavior is relevant to the determination of IPv6 Capability; the internal IPv4 interfaces and the IPv4 legacy devices will not be evaluated, analogous to the internal functions (bus, memory, etc) of any device or set of devices being evaluated as a unit under test for IPv6 Capability.

Systems MAY use other approaches to transition defined in RFCs or Internet-Drafts, as long as they do not conflict or interfere with other requirements for IPv6 Capable Nodes. RFC 3053, IPv6 Tunnel Broker MAY be deployed to support automatic IPv6-in-IPv4 tunneling from dual-stacked hosts to a tunnel broker server. All Routers and L3 Switches serving as Provider Edge Router SHOULD support IPv6 over MPLS following RFC 4798, Connecting IPv6 islands over IPv4 MPLS using IPv6 Provider Edge (6PE) routers.

Additional mechanisms built on top of these existing mechanisms MAY be supported. An example of this is turning a communications gateway server, such as an e-mail server, into a dual-stacked Application-Level Gateway (ALG) that can intermediate between IPv4-only mail clients and IPv6-only mail clients.

2.4 Quality of Service (QoS) Functional Requirements

As IPv6 Quality of Services (QoS) extensions and usage guidance matures, this profile will be expanded. The following are current IPv6 protocols related to QoS signaling:

- RFC 2474, Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
 - Routers MUST process DiffServ headers and offer differentiation of traffic service classes

¹¹ See Internet Draft “Reasons to move NAT-PT to Historic Status”, Auon and Davies (draft-ietf-v6ops-natpt-to-historic-00)

- Routers to be deployed in an Integrated Services (IntServe) architecture SHOULD+ support RSVP based QoS as defined in the following RFCs:
 - RFC 2205, Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification
 - RFC 2207, RSVP Extensions for IPSEC Data Flows
 - RFC 2210, The Use of RSVP with IETF Integrated Services
 - RFC 2750, RSVP Extensions for Policy Control
- Optionally, Routers may also support RFC 3175, Aggregation of RSVP for IPv4 and IPv6 Reservations

2.5 Mobility (MOB) Functional Requirements

Mobile IPv6 (MIPv6) and NEtwork MObility (NEMO) are emerging IPv6-based network mobility services that SHOULD be implemented on new IPv6 systems. Application and deployment conditions will dictate whether these optional features are required for particular configurations, so these requirements are conditional: if a capability is included, the product MUST implement it as defined in the RFCs cited for that capability. MIPv6 is defined in RFC 3775, Mobility Support in IPv6 and security for MIPv6 is defined in RFC 3776, Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents. NEMO is defined in RFC 3963, Network Mobility (NEMO) Basic Support Protocol.

RFC 3776 has recently been updated by RFC 4877, Mobile IPv6 Operations With IKEv2 and the Revised IPsec Architecture. RFC 3776 specified IKEv1 for MIPv6 security while RFC 4877 provides compatibility with the RFC 4301 IPsec architecture by specifying the use of IKEv2 with MIPv6. RFC 4877 will be added to the DISR database as an Emerging standard in the next update cycle, however where practical, we recommend that MIPv6 Capable Nodes and Home Agent Routers support IKEv2 for MIPv6 security.

2.5.1 MIPv6 Capable Node

An End Node which can operate as a Mobile IPv6 node is “MIPv6 Capable”. If a product will be deployed as a MIPv6 Capable Node it MUST support the Mobile Node requirements in RFC 3775, and MUST support RFC 3776. A MIPv6 Capable Node SHOULD+ support RFC 4282, The Network Access Identifier and SHOULD+ support RFC 4283, Mobile Node Identifier Option for MIPv6.

2.5.2 Home Agent Router

The MIPv6 architecture defines a “Home Agent” as a Router on the Mobile Node home network which coordinates the rerouting of packets addressed to the Mobile Node. A Router that will be deployed as a Home Agent MUST support the Home Agent requirements in RFC 3775, and MUST support RFC 3776 and SHOULD+ implement RFC 4282 and RFC 4283.

2.5.3 NEMO Capable Router

Network Mobility (NEMO) extends Mobile Node capability to an entire sub-network. A Router which meets the requirements for Network Mobility is a “NEMO Capable Router.” A NEMO Capable Router MUST implement RFC 3963.

2.5.4 Route Optimization

Any IPv6 Capable Nodes can interoperate with a MIPv6 Mobile Node as a Correspondent Node as stated in Section 8.1 of RFC 3775 (no additional functionality is required.), MIPv6 includes a feature called “Route Optimization” which increases the efficiency of packet routing between a Mobile Node and Correspondent Node. An IPv6 Capable Node to be deployed where MIPv6 is prevalent SHOULD support Route Optimization as defined in RFC 3775.

2.6 Bandwidth Limited Networks Functional Requirements

IPv6 support for RF wireless systems and other bandwidth limited deployments will benefit from optimizations including header compression. The requirements in this section are conditional; where header compression is needed, the listed RFCs MUST be followed. Please note that header compression by its nature may not be compatible with IPsec in some configurations.

2.6.1 Robust Header Compression (RoHC)

Robust Header Compression (RoHC) is designed to provide a significant improvement in transmission efficiency for bandwidth limited networks. It will likely be used in cellular networks (2.5G and 3G) and other wireless links. It is an emerging technology, and where it is used the following RFCs MUST be supported

- RFC 3095, RObust Header Compression (ROHC) – Supports reliable IP header compression over wireless links. When header compression over wireless links is required ROHC MUST be used.¹²
- RFC 3241, RObust Header Compression (ROHC) over PPP - Supports compression over wireless PPP links requiring header compression. ROHC MAY be used to support compression over various PPP and low-speed links
- RFC 3843, RObust Header Compression (ROHC): A Compression Profile for IP– Additional guidance for extending RFC 3095 for any arbitrary IP header chain. Supports reliable IP header compression over wireless links. When header compression over wireless links is required ROHC MUST be used.
- RFC 4362, RObust Header Compression (ROHC): A Link-Layer Assisted Profile for IP/UDP/RTP - Additional guidance for optimizing RFC 3095 for various link-layers. Supports reliable IP header compression over wireless links.

¹² A recent RFC 4815, Robust Header Compression (RoHC) Corrections and Clarifications to RFC 3095 provides some updates and will be added as an Emerging Standard in DISR 07-3.0.

2.6.2 IP Header Compression

IP Header Compression is an earlier alternative to RoHC. Where IP Header Compression is used, the following RFCs MUST be supported.

- RFC 2507, IP Header Compression, February 1999 (For low-speed wired links requiring compression)
- RFC 2508, Compressing IP/UDP/RTP Headers for Low-Speed Serial Links (For low-speed serial links requiring compression)

2.7 Network Management (NM) Functional Requirements

While the requirements for Network Management are still evolving, SNMP Version 3 (SNMPv3) as defined in Standard 62/RFC 3411, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks is the preferred method of remote management. IPv6 Compatible Nodes that are managed via SNMP MUST support SNMPv3 as defined in RFC 3411.

SNMP implementation is built around a Management Information Base (MIB) defined by several general MIB and protocol RFCs as well as MIB RFCs specific to a node type or specific features. SNMP implementations SHOULD support the MIB specifications appropriate to customer requirements. The general MIB specifications include:

- Standard 62/RFC 3412, Message Processing and Dispatching for the SNMP
- Standard 62/RFC 3413, SNMP Applications.
- RFC 3595, Textual Conventions for IPv6 Flow Label
- RFC 4022, Management Information Base for the Transmission Control Protocol
- RFC 4113, Management Information Base for the User Datagram Protocol
- RFC 4087, IP Tunnel MIB

Other MIBs that may be appropriate to specific products or features include:

- RFC 4293, Management Information Base (MIB) for IP, obsoletes RFC 2465 and 2466 and MUST be supported to provide SNMPv3 management of IPv6 features; these two RFCs have been combined with IPv4 MIBs and updated in RFC 4293 to cover all IP management
- RFC 4295, Mobile IP Management MIB SHOULD be supported for Network Management in MIPv6 environment
- RFC 4807, IPsec Security Policy Database Configuration MIB SHOULD be supported when the IPsec Security Policy Database is used
- RFC 4292, IP Forwarding Table MIB SHOULD be supported

2.8 Routing Protocol Requirements

A Router may be deployed as an Exterior Router (at the network edge) or an Interior Router (in the network core). Router products MAY include both capabilities. Layer 3 Switches MAY include Exterior Router capability.

2.8.1 Interior Router Requirements

An Interior Router **MUST** support RFC 2740, OSPF for IPv6 (OSPFv3). An Interior Router **SHOULD+** support RFC 4552, Authentication/Confidentiality for OSPFv3. An Interior Router **MAY** support other routing protocols as appropriate to the deployed routing architecture.

2.8.2 Exterior Router Requirements

An Exterior Router (BGP gateway) between routing systems **MUST** support:

- RFC 4271, A Border Gateway Protocol 4 (BGP-4)
- RFC 1772, Application of the Border Gateway Protocol in the Internet
- RFC 2545, Use of BGP-4 Multi-protocol Extensions for IPv6 Inter-Domain Routing
- RFC 2858¹³, Multi-protocol Extensions for BGP-4

3 Product Class Profiles

The Product Class Profiles for each of the Product Classes defined in section 1.6 can now be specified in terms of the Functional Requirements defined in Section 2. For a specific product presented for evaluation as IPv6 Capable, the information in Section 1.6 should be used to determine the appropriate Product Class for the product and the corresponding Product Class Profile in the following sections.

Additional Product Classes may be added in the future as new products are developed and presented for evaluation, or these Product Classes may be modified to cover additional products. The following paragraphs provide detailed Profiles for each Product Class.

3.1 IPv6 End Nodes

3.1.1 Host/Workstation Product Class Profile

IPv6 Capable Host/Workstation Products:

- **MUST** implement the Base Requirements (Section 2.1);
 - And **MUST** implement RFC 3810, MLDv2;
 - And **SHOULD+** support RFC 3315, DHCPv6 autoconfiguration;
- **MUST** be IPsec Capable, implementing the IPsec Functional Requirements (Section 2.2);
 - And **SHOULD+** support RFC 3041, Privacy Extensions;
 - Conditionally, Hosts/Workstations that will operate on networks requiring privacy address extensions **MUST** follow RFC 3041 when using SLAAC;

¹³ Recently obsoleted by RFC 4760

- Conditionally, MUST support Transition Mechanism (Section 2.3) requirements for Dual Stack capability IF intended deployment requires interoperation with IPv4-only legacy nodes;
- MAY support QoS Functional Requirements (Section 2.4);
- Conditionally, MUST implement Correspondent Node (CN) with Route Optimization (Section 2.5.4) IF intended deployment requires interoperation with MIPv6 Capable Nodes;
- Conditionally, MUST implement MIPv6 Capable Node Functional Requirements (Section 2.5.1) IF intended to be deployed as a Mobile Node;
- MUST implement Standard 66/RFC 3986, Uniform Resource Identifier (URI): Generic Syntax;
- MUST be capable of using IPv6 DNS Resolver function per RFC 3596, DNS Extensions to Support IPv6;
- MUST implement RFC 3484, Default Address Selection for IPv6. It is expected that IPv6 nodes will need to deal with multiple addresses. Section 2.1 of RFC 3484 requires a default “policy table” and encourages implementations to allow manual configuration. Host/Workstation nodes SHOULD+ provide a user configurable policy table to enable override of Default Address Selection (i.e. to force use of specific address in certain situations.)¹⁴

3.1.2 Network Appliance Product Class Profile

IPv6 Capable Network Appliances:

- MUST implement the Base Requirements (Section 2.1);
- SHOULD+ be IPsec Capable by supporting the IPsec Functional Requirements (Section 2.2);
- SHOULD support the complete Host/Workstation profile if possible.

While it is preferable that all IPv6 Capable Products interoperate with IPv4-Only legacy nodes and networks, a Network Appliance MAY be IPv6-Only and therefore rely upon external methods (tunneling or translation) to interoperate with IPv4.

3.1.3 Server Product Class Profiles

3.1.3.1 Advanced Server Profile

IPv6 Capable Advanced Servers:

- MUST implement the Base Requirements (Section 2.1);
 - And MUST implement RFC 3810, MLDv2;

¹⁴ This recommendation is under consideration for upgrade to a MUST. Implementations with configurable policy tables are strongly recommended, and where possible, choose to use operating systems that support a configurable policy table.

- MUST be IPsec Capable, implementing the IPsec Functional Requirements (Section 2.2);
 - And SHOULD+ support RFC 3041, Privacy Extensions;
 - Conditionally, Advanced Servers that will operate on networks requiring privacy address extensions MUST follow RFC 3041 when using SLAAC;
- Conditionally, MUST support Transition Mechanism (Section 2.3) requirements for Dual Stack capability IF intended deployment requires interoperation with IPv4-only legacy nodes;
- MAY support QoS Functional Requirements (Section 2.4);
- Conditionally, MUST implement Correspondent Node (CN) with Route Optimization (Section 2.5.4) IF intended deployment requires interoperation with MIPv6 Capable Nodes;
- MUST implement Standard 66/RFC 3986, Uniform Resource Identifier (URI): Generic Syntax;
- MUST be capable of using IPv6 DNS Resolver function per RFC 3596, DNS Extensions to Support IPv6;
- MUST implement RFC 3484, Default Address Selection for IPv6. It is expected that IPv6 nodes will need to deal with multiple addresses. Section 2.1 of RFC 3484 requires a default “policy table” and encourages implementations to allow manual configuration. Host/Workstation nodes SHOULD+ provide a user configurable policy table to enable override of Default Address Selection (i.e. to force use of specific address in certain situations).¹⁵

A Server will add services according to the manufacturer’s service profile and the deployment requirements for the Server. The full service profile of applications offered by an advanced server is beyond the scope of this document, but should be available from the operating system manufacturer or by referencing industry standard profiles such as the UNIX 03 Standard¹⁶ Linux Base Standard (LSB)¹⁷ or others. Whatever service profile is specified, the IPv6 Advanced Server is expected to offer an IPv6 equivalent of any IPv4 service that the Server is hosting, as well as any IPv6-only services specified in its service profile.

There are many network application services possible, a partial list of services that MAY be provided by a Server include:

- RFC 4330, Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
- RFC 3596, DNS Extensions to Support IPv6

¹⁵ This recommendation is under consideration for upgrade to a MUST. Implementations with configurable policy tables are strongly recommended, and where possible, choose to use operating systems that support a configurable policy table.

¹⁶ <http://www.opengroup.org/openbrand/register/xy.htm>

¹⁷ <http://www.opengroup.org/lsb/cert/register.html>

- RFC 3226, DNS Security and IPv6 Aware Server/Resolver Message Size Requirements
- RFC 3261, Session Initiation Protocol (SIP)
- RFC 3315, Dynamic Host Configuration Protocol for IPv6 (DHCPv6)
- RFC 3053, IPv6 Tunnel Broker
- RFC 3162, RADIUS (Remote Authentication Dial In User Service) and IPv6
- RFC 2911, Internet Printing Protocol (IPP)
- RFC 2821, Simple Mail Transfer Protocol (SMTP)
- RFC 2428, FTP Extensions for IPv6 and NATs; Server must be capable of transferring files with IPv6 and support Extended Data Port (EPRT) and Extended Passive (EPSV) commands
- Standard 9/RFC 959, File Transfer Protocol (FTP)

3.1.3.2 Simple Server Profile

IPv6 Capable Simple Servers:

- MUST implement the Base Requirements (Section 2.1)
- SHOULD+ be IPsec Capable, supporting the IPsec Functional Requirements (Section 2.2);
- SHOULD meet the Advanced Server Profile if possible (section 3.1.3.1);
- Provide at least one network service as discussed in Section 3.1.3.1.

3.2 IPv6 Intermediate Nodes

3.2.1 Router Product Profile

IPv6 Capable Routers:

- MUST implement the Base Requirements (Section 2.1)
 - And MUST implement RFC 3810, MLDv2;
- MUST be IPsec capable, implementing the IPsec Functional Requirements (Section 2.2)
 - And SHOULD support RFC 3041, Privacy Extensions;
 - And MUST support RFC 4302 (AH) to secure routing protocols;¹⁸
- MUST, at a minimum, support Dual Stack and manual tunneling Transition Mechanisms (Section 2.3)
- MUST support RFC 2784, Generic Router Encapsulation (GRE): IPv6-in-IPv4 tunnels and IPv4-in-IPv6 tunnels
- MUST support RFC 2473, Generic Packet Tunneling in IPv6 Specification

¹⁸ This is to be consistent with the DISA FSO Backbone Transport Services (BTS) Security Technical Implementation Guide (STIG) which states the following: "(BTS-RTR-010: CAT II) The router administrator will ensure neighbor authentication with MD5 or *IPv6 AH is implemented for all routing protocols* with all peering routers within the same autonomous system as well as between autonomous systems."

- MUST support the QoS Functional Requirements (Section 2.4)
- Conditionally, A Router MUST implement Home Agent capability as defined in Section 2.5.2 IF it will be deployed as a Home Agent Router;
- Conditionally, A Router MUST implement MIPv6 Network Mobility (NEMO) capability as defined in Section 2.5.3 IF it will be deployed as a NEMO Capable Router.
- MUST support the Network Management Functional Requirements (Section 2.7)
- Conditionally, IF the router functions as an Interior Router (network core) it MUST support the Interior Router Requirements (Section 2.8.1)
- Conditionally, IF the router functions as an Exterior Router (BGP gateway) between routing systems, it MUST support the Exterior Router Requirements (Section 2.8.2)

Note on multicast routing protocols: Multicast routing protocols have recently emerged from the IETF Protocol Independent Multicast (PIM) Working Group as Proposed Standards. RFC 4601, Protocol Independent Multicast – Sparse Mode (PIM-SM) and RFC 3973, Protocol Independent Multicast – Dense Mode (PIM-DM) conditionally **SHOULD+** be implemented IF deployment requires multicast routing protocols.

3.2.2 Layer-3 (L3) Switch Product Profile

IPv6 Capable L3 Switches:

- MUST implement the Base Requirements (Section 2.1)
- **SHOULD+** be IPsec Capable, implementing the IPsec Functional Requirements (Section 2.2)
- Conditionally, MUST support the Exterior Router Requirements (Section 2.8.2) IF the product will be used as an exterior system node and must support routing functions to interface with routers at edge of a switching network
- Conditionally, MUST support the Network Management Functional Requirements (Section 2.7) IF the product is a managed switch
- MAY support RFC 4541, Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches

3.2.3 Information Assurance (IA) Device Product Profile

IPv6 Capable IA Devices:

- MUST implement the Base Requirements (Section 2.1)
- Conditionally, MUST be IPsec Capable, implement the IPsec Functional Requirements, IF the device is an IPsec based in-line network encryptor (INE), VPN server, or if it must exchange information with other devices across IPsec secured connections. Some instances of intrusion detection devices, simple firewalls, and other security devices may simply monitor traffic flows and not actually send/receive data across the network and may not require IPsec.

- High security requirements for classified networks encryption MAY include encryption transforms and algorithms not necessarily interoperable with standard IPsec. These devices SHOULD+ support the complete IPsec Functional Requirements but MAY support a minimal subset of the IPsec requirements:
 - RFC 4301, Security Architecture for the Internet Protocol
 - RFC 4303, IP Encapsulating Security Payload (ESP)
 - Manual Keying
- If a security device must distribute IP Security Policy information to other devices, it SHOULD+ implement:
 - RFC 3585, IPsec Configuration Policy Information Model
 - RFC 3586, IP Security Policy Requirements
 - Note: New Security device standards are emerging for managing IPsec policy information, managing distributed firewalls, etc., which will fit in this category. There is no official DoD IPv6 IPsec policy available at this time.
- Devices MUST also support IPv6 requirements defined for any special security function of the device. Example:
 - Remote Authentication Dial In User Service (RADIUS) authentication servers MUST support RFC 3162, Remote Authentication Dial In User Service (RADIUS) and IPv6

3.2.3.1 Integrated Security Device (ISD) Additional Requirements

An Integrated Security Device (ISD) is a device that performs stateful packet inspection of both the IPv4 and IPv6 protocols and performs Intrusion Prevention and Intrusion Detection functions (IPS/IDS) within the same device on both IPv4 and IPv6 protocol stacks.

- An IPv6 Capable ISD MUST support the Information Assurance Device Profile requirements
- The ISD product MUST be able to use BOTH predefined and custom defined threat signatures to detect and prevent intrusion attempts.

3.2.3.2 IPv6 Security Proxy Additional Requirements

An IPv6 Security Proxy is a device or appliance that is designed to terminate a session and initiate a session on the behalf of an IPv6 host. An IPv6 Proxy also serves as a network segregator for services and applications. A Proxy Appliance has a scalable proxy platform architecture to secure Web communications and accelerate delivery of business applications.

- An IPv6 Security Proxy MUST support the Information Assurance Device Profile Requirements.
- An IPv6 Security Proxy is limited to Tunnel Mode IPsec, and MUST NOT provide Transport Mode IPsec.

4 IPv6 Capable Software

We anticipate that software products will be presented for evaluation as IPv6 Capable, but the requirements for IPv6 Capable software are limited. Further analysis is needed to develop Product Class definitions for software products, but this section is included to document the current state of the discussion on requirements for Software products.

Software products can be divided into Operating System products and Application products, with the following definitions:

Operating System (OS): The foundational software on a Host/Workstation or Server that provides an environment for running applications. The OS includes the communications software (drivers) that provide the IPv6 capabilities and an Application Programming Interface (API) that allows IPv6 Capable Applications to use these features.

Application: Software expressing specific functional requirements, particular to its use. The evaluation of an Application software product as IPv6 Capable is based on its use of IPv6 addresses and other IPv6-specific features available through the API.

4.1 Application Programming Interface (API) Characteristics

All applications on Hosts/Workstations, Network Servers or Network Appliances that require IP network protocol service MUST use IPv6 Capable versions of those network protocols. These include the basic and extended specifications of the Socket API as appropriate to the application architecture¹⁹. Applications will require evaluation and testing for approval as IPv6 capable as components of a system under test (embedded software) or as a stand-alone product.

Application Vendors can be expected to scan and test their code for IPv6 compliance and provide a letter of compliance indicating to what degree they comply. End users of Applications will be looking to DISA to verify that the Application will interoperate with other IPv6 components based on the DISR profiles. Third party or packaged Applications may be considered COTS if they have already been submitted by the vendor, tested and on the Approved Product List (APL). Embedded or custom applications as well as unevaluated vendor Applications (i.e. not on APL) will be subject to testing.

General purpose Operating Systems can be considered COTS components, if previously submitted by the vendor, tested, and on the APL. This will limit the scope of testing to verifying IPv6 compliance of IPv6-specific requirements upon the application itself in these cases. In cases where the Application under test includes a proprietary or

¹⁹ The Socket API extensions are defined in Informational RFCs, as they would not apply to all applications, i.e. those that use other operating system methods for networking.

customized Operating System, the test plan may also address the IPv6 functional requirements on the operating system.

In reality, an Application and Operating System cannot be tested in isolation; some level of integration testing will be achieved when exercising the two components. Novel combinations of previously approved COTS Applications and Operating Systems may be subjected to Integration Testing, but in general that would be an end-user responsibility.

There are currently no generic requirements for an IPv6 Capable application beyond the API RFCs:

- RFC 3493, Basic Socket Interface Extensions for IPv6
- RFC 3542, Advanced Sockets Application Program Interface (API) for IPv6
- On MIPv6 Capable Nodes, for some Mobile applications, RFC 4584, Extension to Sockets API for Mobile IPv6

In addition, specific requirements may be needed for various classes of applications including:

1. File Transfer Protocol (FTP) client
2. Web Browser
3. E-mail client
4. IM client

4.2 Software Requirements

IPv6 Capable Operating Systems MUST support Dual Stack and MUST support both IPv4 and IPv6 applications in the Application Program Interface (APIs).

Evaluation of an Application software product as IPv6 Capable is limited to its ability to send and receive IPv6 packets with an IPv6 client, and its use of IPv6 addresses and features available through the API.

Appendix A: References

The primary source for requirements cited in this document is the body of Internet Engineering Task Force (IETF) specifications known as “Request For Comment” (RFC) which are referenced throughout the document. These references can be found through <http://www.ietf.org/> by using the RFC Search feature on the RFC Editor page. The Requirements Summary Table (Appendix C) can be used as a cross-reference for the RFCs cited as requirements in this document.

The following additional sources were used in generating requirements for this document:

- [1] “Internet Protocol Version 6 (IPv6) Interim Transition Guidance” John Stenbit, CIO US Department of Defense; September 23, 2003
- [2] “Internet Protocol Version 6 (IPv6)” DoD CIO Memorandum; June 9, 2003
- [3] DoD Information Technology Standards Registry (DISR); a repository of cited standards to be followed by DoD projects and deployments. This database can be accessed by authorized users via the web at <https://disronline.disa.mil/>
- [4] “Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Draft IPv6 Capable Functional Specification v1.0” November 22 2005
- [5] “Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Information Assurance (IA) Solutions Version 1.0” September 8, 2005
- [6] Memorandum for Department of Defense Executive Agent for Information Technology Standards regarding DISR Baseline Release 06-02; June 27, 2006. This Memorandum linked Version 1.0 of the Standard Profiles document to the DISR baseline, and stated that the Standard Profiles document was approved as guidance in the procuring/acquisition of IPv6 Capable Products. We anticipate that a similar Memorandum will be issued when Version 2.0 is approved.
- [7] NIST Communications Security Establishment document “FAQ for the Cryptographic Module Validation Program” updated December 8, 2006 <http://csrc.nist.gov/cryptval/140-1/CMVPFAQ.pdf>
- [8] Memorandum for Secretaries of the Military Departments, et al “Internet Protocol Version 6 (IPv6) Policy Update” issued by Assistant Secretary of Defense – Networks and Information Integration, August 16, 2005
- [9] NIST Special Publication 500-267 “A Profile for IPv6 in the U.S. Government – Version 1.0” draft for public comment, February 22, 2007

- [10] Internet Draft “Deprecation of Type 0 Routing Headers in IPv6” J. Abley et al, May 16, 2007; this is a work in progress, which will update RFC 2460 if approved.
- [11] “The Teredo Protocol: Tunneling Past Network Security and Other Security Implications” Dr. James Hoagland, Symantec Report
http://www.symantec.com/avcenter/reference/Teredo_Security.pdf
- [12] Department of Defense (DoD) Internet Protocol Version 6 (IPv6) Transition Office (DITO) Information Assurance (IA) Guidance for Milestone Objective 2 (MO2) Version 1.1
- [13] DISA FSO Backbone Transport Services (BTS) Security Technical Implementation Guide (STIG)
<http://iase.disa.mil/stigs/index.html>

Appendix B: Glossary

This glossary is provided for the convenience of the reader, and is intended to include terminology and acronym definitions specific to this document, plus other terms in general use.

IPv6: The Internet Protocol Version 6; a replacement for the widely deployed Internet Protocol Version 4. IPv6 and related protocols are defined by IETF in RFCs which can be found at <http://www.ietf.org/>. Basic information on IPv6 can be found at <http://en.wikipedia.org/wiki/IPv6> or through [the North American IPv6 Task Force](#).

IETF: The Internet Engineering Task Force is a large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the Internet. It is open to any interested individual. The IETF Mission Statement is documented in [RFC 3935](#). More information can be found at <http://www.ietf.org/>.

RFC: Request for Comment; for historical reasons, publications of the IETF are called Requests for Comment, but everyone just calls them RFCs. When an Internet-Draft is accepted for publication, the RFC Editor assigns a number which permanently identifies the publication. Thus any RFC cited can be found by number through the [RFC Editor](#).

IPv6 Capable: According to the IPv6 Interim Transition Memorandum [1] an “IPv6 Capable” system or product shall be capable of receiving, processing and forwarding IPv6 packets and/or interfacing with other protocols in a manner similar to IPv4. Specific criteria for determining whether a product is an IPv6 Capable Product is defined by this document.

IPv6 Capable Product: The term “IPv6 Capable Product”, as used in this document, is any product that meets the minimum set of mandated requirements, appropriate to its Product Class, necessary for it to interoperate with other IPv6 products employed in DoD IPv6 networks. Thus an IPv6 Capable Product is one that meets the IPv6 Capable requirements specific to the Product Profile for the Product Class appropriate for the product.

Product Class: as used in this document a Product Class is one of a set of definitions used in this document to group products with common characteristics and requirements.

Appendix C: Requirements Summary Table

The Requirements Summary Table list RFC numbers and notes on their applicability to each Product Class.

RFC Status: Info – Informational; PS – Proposed Standard; DS – Draft Standard; STD – Approved Standard; BCP – Best Current Practice; OBS – Obsolete; HIST – Historic; EXP – Experimental

Applicability: M – MUST; S+ – SHOULD+; S – SHOULD; O – Optional (MAY); C – Conditional (followed by another code, for example C M indicates Conditional MUST); I – Informational; SN – SHOULD NOT; MN – MUST NOT

| Functional Requirements Section | | RFC | | | Applicability by Product Class | | | | | | | |
|---------------------------------|-------------------------|-----------------|--|-----------------------------|--------------------------------|-----------------|-----------------|-----------------|-----------------|-----------------|-----------------|---|
| Number | Title [sub-topic] | Number [subset] | Title [sub-topic] | Status | Host | Net App | Adv Server | Simple Server | Router | L3 Switch | IA Device | |
| 2.1 | Base Requirements | 2460 | Internet Protocol, Version 6 (IPv6) Protocol Specification | DS | M | M | M | M | M | M | M | |
| | | 4443 | Internet Control Message Protocol (ICMPv6) | DS | M | M | M | M | M | M | M | |
| | | 2461 | Neighbor Discovery for IPv6 | DS | M | M | M | M | M | M | M | |
| | | 1981 | Path MTU Discovery for IPv6 | DS | M | S | M | S | M | M | M | |
| | [address configuration] | 2462 | IPv6 Stateless Address Auto-configuration (SLAAC) | DS | M ²⁰ | M ²⁰ | M ²⁰ | M ²⁰ | M ²⁰ | M ²⁰ | M ²⁰ | |
| | | 3315 | DHCPv6 [client] | PS | | | | | | | | |
| | | | n/a | [disable autoconfiguration] | | M | M | M | M | M | M | M |

²⁰ All Product Classes MUST support a method of autonomous configuration, either SLAAC or DHCPv6 client.

| Functional Requirements Section | | RFC | | | Applicability by Product Class | | | | | | |
|---------------------------------|--------------------------------|-----------------|---|--------|--------------------------------|---------|------------|---------------|--------|-----------|-----------|
| Number | Title [sub-topic] | Number [subset] | Title [sub-topic] | Status | Host | Net App | Adv Server | Simple Server | Router | L3 Switch | IA Device |
| | [address architecture] | 4291 | IPv6 Addressing Architecture | DS | M | M | M | M | M | M | M |
| | | 4007 | Scoped Address Architecture | PS | M | M | M | M | M | M | M |
| | | 4193 | Unique Local IPv6 Unicast Addresses | PS | M | M | M | M | M | M | M |
| | [Multicast listener discovery] | 2710 | Multicast Listener Discovery for IPv6 | PS | M | M | M | M | M | M | M |
| | | 3810 | MLDv2 for IPv6 | PS | M | S | M | S | M | M | S |
| | [connection technology] | 2464 | IPv6 over Ethernet | PS | C M | C M | C M | C M | C M | C M | C M |
| | | 2492 | IPv6 over ATM | PS | C M | C M | C M | C M | C M | C M | C M |
| | | 2472 | IPv6 over PPP | PS | C M | C M | C M | C M | C M | C M | C M |
| | | 3572 | IPv6 over MAPOS | PS | C M | C M | C M | C M | C M | C M | C M |
| | | 2467 | IPv6 over FDDI | PS | C M | C M | C M | C M | C M | C M | C M |
| | | 2491 | IPv6 over NBMA | PS | C M | C M | C M | C M | C M | C M | C M |
| | | 2497 | IPv6 over ARCnet | PS | C M | C M | C M | C M | C M | C M | C M |
| | | 2590 | IPv6 over Frame Relay | PS | C M | C M | C M | C M | C M | C M | C M |
| | | 3146 | IPv6 over IEEE 1394 Networks | PS | C M | C M | C M | C M | C M | C M | C M |
| | | 4338 | IPv6, IPv4 and ARP Packets over Fibre Channel | PS | C M | C M | C M | C M | C M | C M | C M |

| Functional Requirements Section | | RFC | | | Applicability by Product Class | | | | | | |
|---------------------------------|-------------------|-----------------|--|--------|--------------------------------|---------|------------|---------------|--------|-----------|-----------|
| Number | Title [sub-topic] | Number [subset] | Title [sub-topic] | Status | Host | Net App | Adv Server | Simple Server | Router | L3 Switch | IA Device |
| 2.2 | IPsec | 4301 | Security Architecture for the Internet Protocol | PS | M | S+ | M | S+ | M | S+ | C M |
| | | 4302 | IP Authentication Header | PS | S | S | S | S | M | S | S |
| | | 4303 | IP Encapsulating Security Payload | PS | M | S+ | M | S+ | M | S+ | C M |
| | | 4304 | Extended Sequence Number (ESN) Addendum to IPsec Domain of Interpretation (DOI) for Internet Security Association and Key Management Protocol (ISAKMP) | PS | S | S | S | S | S | S | S |
| | | 4305 | Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH) | OBS | M | S+ | M | S+ | M | S+ | C M |
| | | 4869 | Suite B Cryptographic Suites for Ipsec | Info | S+ | S+ | S+ | S+ | S+ | S+ | S+ |
| | | 4309 | Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP) | PS | C S | C S | C S | C S | C S | C S | C S |
| | [SeND] | 3971 | Secure Neighbor Discovery | PS | S | S | S | S | S | S | S |
| | [CGA] | 3972 | Cryptographically Generated Addresses | PS | S | S | S | S | S | S | S |

| Functional Requirements Section | | RFC | | | Applicability by Product Class | | | | | | | |
|---------------------------------|---------------------------|-----------------|--|-----------|--------------------------------|---------|------------|---------------|--------|-----------|-----------|--|
| Number | Title [sub-topic] | Number [subset] | Title [sub-topic] | Status | Host | Net App | Adv Server | Simple Server | Router | L3 Switch | IA Device | |
| | [SLAAC Privacy Extension] | 3041 | Privacy Extensions for Stateless Address Auto configuration in IPv6 | PS | S+ C M | S | S+ C M | S | S+ C M | S | S | |
| 2.2.2 | IKEv2 | 4306 | Internet Key Exchange Version 2 (IKEv2) Protocol | PS | M | S+ | M | S+ | M | S+ | M | |
| | | 4307 | Cryptographic Algorithms for Internet Key Exchange Version 2 (IKEv2) | PS | M | S+ | M | S+ | M | S+ | M | |
| 2.3 | Transition Mechanisms | 4213 | Transition Mechanisms for IPv6 Hosts and Routers [Dual Stack] | PS | C M | S | C M | S | M | O | | |
| | | 4213 | Transition Mechanisms for IPv6 Hosts and Routers [manual tunnels] | PS | | | | | M | O | | |
| | | 4213 | Transition Mechanisms for IPv6 Hosts and Routers [Translation and other methods] | PS | O | O | O | O | O | O | O | |
| | | 4213 | Transition Mechanisms for IPv6 Hosts and Routers [Remainder] | PS | I | I | I | I | I | I | I | |
| | | 2766 | Network Address Translation – Protocol Translation (NAT-PT) | PS (HIST) | SN | SN | SN | SN | SN | SN | SN | |
| | | 3053 | IPv6 Tunnel Broker | INFO | C M | C S | C M | C S | C M | O | | |

| Functional Requirements Section | | RFC | | | Applicability by Product Class | | | | | | | |
|---------------------------------|-------------------|--------------------|---|--------|--------------------------------|---------|------------|---------------|--------|-----------|-----------|--|
| Number | Title [sub-topic] | Number [subset] | Title [sub-topic] | Status | Host | Net App | Adv Server | Simple Server | Router | L3 Switch | IA Device | |
| | [provider edge] | 4798 | Connecting IPv6 islands over IPv4 MPLS using IPv6 Provider Edge (6PE) routers | PS | | | | | O | O | | |
| 2.4 | QoS | 2474 | Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers | PS | O | O | O | O | M | | | |
| | | 2205 | Resource ReSerVation Protocol (RSVP) – Version 1 Functional Specification | PS | O | O | O | O | S+ | | | |
| | | 2207 | RSVP Extensions for IPSEC Data Flows | PS | O | O | O | O | S+ | | | |
| | | 2210 | The Use of RSVP with IETF Integrated Services | PS | O | O | O | O | S+ | | | |
| | | 2750 | RSVP Extensions for Policy Control | PS | O | O | O | O | S+ | | | |
| | | 3175 | Aggregation of RSVP for IPv4 and IPv6 Reservations | PS | O | O | O | O | O | | | |
| 2.5.1 | MIPv6 Capable | 3775 [Mobile Node] | Mobility Support in IPv6 | PS | C M | C S | | | | | | |
| | | 3776 [Mobile Node] | Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents | PS | C M | C S | | | | | | |
| | | 4282 | The Network Access Identifier | PS | C S+ | C S | | | | | | |
| | | 4283 | Mobile Node Identifier for Option for IPv6 | PS | C S+ | C S | | | | | | |

| Functional Requirements Section | | RFC | | | Applicability by Product Class | | | | | | | |
|---------------------------------|--------------------|-------------------|---|--------|--------------------------------|---------|------------|---------------|--------|-----------|-----------|--|
| Number | Title [sub-topic] | Number [subset] | Title [sub-topic] | Status | Host | Net App | Adv Server | Simple Server | Router | L3 Switch | IA Device | |
| 2.5.2 | Home Agent Router | 3775 [Home Agent] | Mobility Support in IPv6 | PS | | | | | C M | | | |
| | | 3776 [Home Agent] | Using IPsec to Protect Mobile IPv6 Signaling between Mobile Nodes and Home Agents | PS | | | | | C S+ | | | |
| | | 4282 | The Network Access Identifier | PS | | | | | C M | | | |
| | | 4283 | Mobile Node Identifier for Option for IPv6 | PS | | | | | C S+ | | | |
| 2.5.3 | NEMO Capable | 3963 | Network Mobility (NEMO) Basic Support Protocol | PS | | | | | C M | | | |
| 2.5.4 | Route Optimization | 3775 (sect 9) | Mobility Support in IPv6 | PS | C M | C S | C M | C S | | | | |
| 2.6.1 | RoHC | 3095 | Robust Header Compression (RoHC) | PS | O | O | O | O | O | O | | |
| | | 3241 | RoHC over PPP | PS | O | O | O | O | O | O | | |
| | | 3843 | RoHC: A Compression Profile for IP | PS | O | O | O | O | O | O | | |
| | | 4362 | RoHC: A Link-Layer Assisted Profile for IP/UDP/RTP | PS | O | O | O | O | O | O | | |

| Functional Requirements Section | | RFC | | | Applicability by Product Class | | | | | | |
|---------------------------------|-----------------------|-----------------|--|--------|--------------------------------|---------|------------|---------------|--------|-----------|-----------|
| Number | Title [sub-topic] | Number [subset] | Title [sub-topic] | Status | Host | Net App | Adv Server | Simple Server | Router | L3 Switch | IA Device |
| 2.6.2 | IP Header Compression | 2507 | IP Header Compression | PS | O | O | O | O | O | O | |
| | | 2508 | Compressing IP/UDP/RTP Headers for Low-Speed Serial Links | PS | O | O | O | O | O | O | |
| 2.7 | Network Management | 3411 | An Architecture for Describing Simple Network Management Protocol Version 3 (SNMPv3) | STD 62 | | | | | M | C M | |
| | | 3412 | Message Processing and Dispatching for the SNMP | STD 62 | | | | | M | C M | |
| | | 3413 | SNMP Applications | STD 62 | | | | | M | C M | |
| | [MIBs] | 3595 | Textual Conventions for IPv6 Flow Label | PS | | | | | M | C M | |
| | | 4022 | Management Information Base for the Transmission Control Protocol | PS | | | | | M | C M | |
| | | 4113 | Management Information Base for the User Datagram Protocol | PS | | | | | M | C M | |
| | | 4087 | IP Tunnel MIB | PS | | | | | M | C M | |
| | | 4293 | Management Information Base (MIB) for IP | PS | | | | | M | C M | |
| | | 4295 | Mobile IP Management MIB | PS | | | | | C M | C M | |

| Functional Requirements Section | | RFC | | | Applicability by Product Class | | | | | | | |
|---------------------------------|---------------------|-----------------|--|--------|--------------------------------|---------|------------|---------------|--------|-----------|-----------|--|
| Number | Title [sub-topic] | Number [subset] | Title [sub-topic] | Status | Host | Net App | Adv Server | Simple Server | Router | L3 Switch | IA Device | |
| | | 4807 | IPsec Security Policy Database Configuration | PS | | | | | C M | C M | | |
| | | 4292 | IP Forwarding Table MIB | PS | | | | | M | C M | | |
| 2.8 | Routing Requirement | 2784 | Generic Router Encapsulation (GRE) | PS | | | | | M | | | |
| | | 2473 | Generic Packet Tunneling in IPv6 | PS | | | | | M | | | |
| | [Multicast] | 4601 | Protocol Independent Multicast – Sparse Mode (PIM-SM) | PS | | | | | C S+ | | | |
| | | 3973 | Protocol Independent Multicast – Dense Mode | PS | | | | | C S+ | | | |
| 2.8.1 | Interior Router | 2740 | OSPF for IPv6 (OSPFv3) | PS | | | | | C M | | | |
| | | 4552 | Authentication/Confidentiality for OSPFv3 | PS | | | | | C S+ | | | |
| 2.8.2 | Exterior Router | 4271 | A Border Gate Protocol (BGP-4) | DS | | | | | C M | C M | | |
| | | 1772 | Application of the Border Gateway Protocol in the Internet | DS | | | | | C M | C M | | |
| | | 2545 | Use of BGP-4 Multi-Protocol Extensions for IPv6 Inter-Domain Routing | PS | | | | | C M | C M | | |
| | | 2858 | Multi-Protocol Extensions for BGP-4 | OBS | | | | | C M | C M | | |

| Functional Requirements Section | | RFC | | | Applicability by Product Class | | | | | | | |
|---------------------------------|-------------------|--------------------|--|--------|--------------------------------|---------|------------|---------------|--------|-----------|-----------|--|
| Number | Title [sub-topic] | Number [subset] | Title [sub-topic] | Status | Host | Net App | Adv Server | Simple Server | Router | L3 Switch | IA Device | |
| 3.1.3.1 | Server [Services] | 959 | File Transfer Protocol | STD 9 | | | O | O | | | | |
| | | 2428 | FTP Extensions for IPv6 and NAT | PS | | | O | O | | | | |
| | | 2821 | Simple Mail Transfer Protocol (SMTP) | PS | | | O | O | | | | |
| | | 2911 | Internet Printing Protocol | PS | | | O | O | | | | |
| | | 3162 | RADIUS (Remote Authentication Dial-In User Service) and IPv6 | PS | | | O | O | | | C M | |
| | | 4330 | Simple Network Time Protocol (SNTP) | INFO | | | O | O | | | | |
| | | 3226 | DNS Security and IPv6 A6 Aware Server/Resolver Message Size Requirements | PS | | | O | O | | | | |
| | | 3261 | Session Initiation Protocol (SIP) | PS | | | O | O | | | | |
| | | 3596 | DNS Extensions to Support IPv6 | DS | | | O | O | | | | |
| 3.1.1 | Host | 3484 [Sec 2.1] | Default Address Selection for IPv6 [Policy Table] | PS | S+ | S | S+ | S | | | | |
| | | 3484 [rest of RFC] | Default Address Selection for IPv6 | PS | M | S | M | S | | | | |
| | | 3596 [resolver] | DNS Extensions to Support IPv6 | DS | M | S | M | S | | | | |

| Functional Requirements Section | | RFC | | | Applicability by Product Class | | | | | | | |
|---------------------------------|-------------------|-----------------|---|--------|--------------------------------|---------|------------|---------------|--------|-----------|-----------|--|
| Number | Title [sub-topic] | Number [subset] | Title [sub-topic] | Status | Host | Net App | Adv Server | Simple Server | Router | L3 Switch | IA Device | |
| | | 3986 | Uniform Resource Identifier (URI): Generic Syntax | STD 66 | M | S | M | S | | | | |
| 3.2.3 | IA Device | 3585 | IPsec Configuration Policy Information Model | PS | | | | | | | C S+ | |
| | | 3586 | IP Security Policy Requirements | PS | | | | | | | C S+ | |

1 Acknowledgements

^A *UNIX is a registered trademark of The Open Group*

^B *Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.*

^C *Windows is a registered trademark of Microsoft Corporation in the United States and other countries.*

ERRATA**Errata Issued For DoD IPv6 Standard Profiles For IPv6 Capable Products
Version 2.0, dated 01 August 2007**

Page 35, Appendix C: Requirements Summary Table: RFC 3810, MLDv2 for IPv6, L3 Switch Requirement: Change "M" to "S".

RATIONALE: This editorial change correctly reflects the MLDv2 requirements of paragraph 2.1, Base Requirements.

Issued by: DISR IPv6 Standards Technical Working Group
POC: Ralph Liguori, Chair IPv6 Standards TWG
E-mail Address: ralph.liguori@disa.mil